




Ejercicio Práctico

 **Título:** Redacción Profesional de Múltiples Hallazgos de Seguridad en un Entorno Simulado

Objetivo del ejercicio:

Aplicar los principios de **claridad, precisión, priorización y acción orientada** para redactar un fragmento de informe profesional que incluya **múltiples hallazgos de seguridad**, evidencias técnicas y recomendaciones clasificadas por criticidad.

Escenario:

Tu equipo de ciberseguridad ha realizado una auditoría técnica a una aplicación web de una entidad pública. Se han detectado tres vulnerabilidades:

1. **Uso de contraseña por defecto ("admin/admin")** en el panel de administración.
2. **Página de login expone trazas internas** al ingresar credenciales inválidas.
3. **La API pública no tiene autenticación para solicitudes GET de datos sensibles.**

El director de TI ha solicitado un informe profesional que incluya los hallazgos, evidencias resumidas y recomendaciones viables, estructurado con claridad para un comité mixto (técnicos y gerenciales).

Actividad:

Desarrolla un extracto de informe técnico siguiendo el siguiente formato:

Formato sugerido:

1. Título del informe
 2. Introducción breve (3–4 líneas)
 3. Tabla de Hallazgos (incluye título del hallazgo, impacto, criticidad, recomendación)
 4. Redacción técnica detallada de UNO de los hallazgos, con evidencia y recomendación expandida
-

Modelo de tabla a completar:

Hallazgo	Impacto	Criticidad	Recomendación
Uso de credenciales por defecto	Acceso administrativo no autorizado	Alta	Cambiar credenciales y reforzar políticas de autenticación
Exposición de trazas internas	Revelación de rutas, clases y lógica interna del sistema	Media	Configurar manejo de errores personalizado
API sin autenticación	Acceso libre a datos sensibles	Alta	Implementar autenticación y control de acceso

Desarrollo del punto 4 (por ejemplo, redactar el hallazgo de la API pública):

Incluye:

- Herramienta utilizada para descubrir la vulnerabilidad
 - Método de prueba aplicado
 - Evidencia resumida (respuesta, código, error, etc.)
 - Recomendación técnica detallada
-

Requisitos:

- Usa lenguaje profesional, directo y preciso
- Prioriza la estructura y la acción técnica
- No uses textos genéricos o decorativos